CHESHAM TOWN COUNCIL

INFORMATION TECHNOLOGY POLICY

STATEMENT OF PURPOSE

Many workplaces allow staff personal use of information technology (IT), including email and the internet. Chesham Town Council acknowledges that reasonable use of these technologies at work assists staff with their work-life balance by enabling them to make personal arrangements quickly and efficiently. However, it is necessary to prevent abuse of the system and protect IT equipment from malicious software.

It is important to formalise this arrangement so that the employer and all employees have a clear understanding of what activities are and are not allowed.

POLICY COVERAGE

This policy applies to:

- employees
- Chesham Town Council computer equipment
- Volunteers using Chesham Town Council computer equipment
- Members when using Chesham Town Council computer equipment
- Members using social networking media in their capacity as Councillors

POLICY STATEMENT

Personal use of Chesham Town Council computer equipment is permitted, but should be kept to a minimum during working hours.

All computers used to send/receive emails, access the internet or access the Town Council's IT systems must have recognised up-to-date antivirus software installed. Employees/Members/Volunteers using Town Council equipment must not download files from the internet, email, memory stick or disc without implementing virus protection measures. All employees/Members/volunteers must report any virus problems immediately to their supervisor or IT contractor, as appropriate.

In specific circumstances, volunteers may be given access to the Town Council's IT systems, e.g. work experience students. It is the responsibility of the supervising

member of staff to explain acceptable usage to volunteers.

Chesham Town Council Internet Usage:
Browsing offensive or pornographic websites is prohibited.
Pornographic or offensive material must not be downloaded from the internet.
Indecent remarks, proposals or materials must not be posted on the internet.
Malicious software (including logic bombs, Trojan horses, viruses and worms) must not be knowingly downloaded from the internet.
Confidential information must not be posted on the internet.

Wireless Internet Access
Members of the public who hire rooms at the Town Hall can also pay to access the Town Hall's wireless internet service. Hirers must agree to sign up to the following set of conditions before being given access to the internet:

Browsing offensive or pornographic websites is prohibited.
Pornographic or offensive material must not be downloaded from the internet.
Indecent remarks, proposals or materials must not be posted on the internet.
Malicious software (including logic bombs, Trojan horses, viruses and worms) must not be knowingly downloaded from the internet.
If using the Town Council's laptop, the antivirus must be enabled at all times.

Wireless internet access is controlled by a password which can be changed by the Town Hall officers at any time.

Email:
Employees/Members must not solicit, send or willingly receive emails of an obscene nature, or which are intended to annoy, harass, intimidate or cause offence to colleagues or members of the public.

Personal or sensitive data must not be sent via email unless agreement has been received from the individual concerned or this processing is necessary to carry out public functions.

Council officers should regularly delete or archive emails when they are no longer current or required in order to restrict the size of their mailboxes and reduce the risk of incoming emails being rejected.

Officers should be aware of the characteristics of spam and phishing emails and should not reply to these emails, but add the sender to their email system's Blocked Senders List.

Emails sent by employees must have one of the following disclaimers (as appropriate):

Elgiva:
"Any opinions expressed in this email are those of the individual and are not necessarily those of Chesham Town Council. This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the recipient, the use of the information by disclosure, copying or distribution is prohibited and may be unlawful. If you have received this email in error please notify the administration manager at admin@elgiva.com.

Alternatively please contact the Elgiva Theatre at St Mary's Way, Chesham HP5 1HR.

Chesham Town Council has scanned this email and attachments for viruses but does not accept any responsibilities for viruses once this email has been transmitted. The recipient is responsible for scanning emails and any attachments for viruses themselves."

Town Hall/Parks & Premises/Open Air Pool:
"Any opinions expressed in this email are those of the individual and are not necessarily those of Chesham Town Council. This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the recipient, the use of the information by disclosure, copying or distribution is prohibited and may be unlawful. If you have received this email in error please notify the administration manager at admin@chesham.gov.uk.

Alternatively please contact the Town Council at Chesham Town Hall, Chesham HP5 1DS.

Chesham Town Council has scanned this email and attachments for viruses but does not accept any responsibilities for viruses once this email has been transmitted. The recipient is responsible for scanning emails and any attachments for viruses themselves."

Social Networking
Social networking media, including Facebook, Twitter and blogs may be used by the Town Council as part of its means of communication with residents and service users. Such media will be used to represent the Council as a corporate body. Where members of the public are able to post to a social media page representing the Town Council, the pages will be monitored by Town Council officers to ensure that any offensive, inappropriate or discriminatory messages will be deleted.

Members who use social networking sites in their capacity as councillors must make it clear that they are speaking in a personal capacity and not representing the view of the Council. It is the responsibility of Members to ensure that they are adhering to the Council's Code of Conduct when using social networking sites.

CONFIDENTIALITY & DATA PROTECTION

Employees/Members must not reveal or publicise to a third party confidential or proprietary information, which includes, but is not limited to: personal or sensitive data as defined under the Data Protection Act (1998), computer software source codes, logins, or passwords, unless they have the permission of the Town Clerk or it is in accordance with the Data Protection Act.

Employees who have remote access to the Town Council's IT systems are responsible for ensuring that non-employees do not gain access to the systems.

Chesham Town Council respects the privacy and autonomy of its employees and Members.

MONITORING

Chesham Town Council currently does not monitor the emails or internet usage of its officers. However, monitoring may be employed under the following circumstances:

- complaints are received about malicious emails
- evidence of criminal activity or sending/downloading pornographic images
- staff are spending unreasonable amounts of time visiting non-work related internet sites or sending personal emails

Before monitoring is undertaken, all staff would be informed and provided with information on Chesham Town Council's approach to monitoring. Any monitoring would comply with the Data Protection Act and information obtained from monitoring would only be used for the purpose it was obtained.

DISCIPLINARY PROCEDURES

If an employee breaches the IT policy, they will be subject to the Council's disciplinary procedures. Breaches of the IT Policy by Members could contravene the Code of Conduct and action may result from this contravention.

POLICY REVIEW

Chesham Town Council is committed to reviewing its policies and making improvements where possible.

Adopted: 12 December 2011
Policy Due for Review: December 2015